Mutually Unbiased Bases are Complex Projective 2-Designs

Andreas Klappenecker
Department of Computer Science
Texas A&M University
College Station, TX, 77843–3112, USA
Email: klappi@cs.tamu.edu

Martin Rötteler
NEC Labs America, Inc.
4 Independence Way
Princeton, NJ 08540 U.S.A.
Email: mroetteler@nec-labs.com

***Abstract*— Mutually unbiased bases (MUBs) are a primitive used in quantum information processing to capture the principle of complementarity. While constructions of maximal sets of $d+1$ such bases are known for system of prime power dimension d, it is unknown whether this bound can be achieved for any non-prime power dimension. In this paper we demonstrate that maximal sets of MUBs come with a rich combinatorial structure by showing that they actually are the same objects as the complex projective 2-designs with angle set $\{0, 1/d\}$. We also give a new and simple proof that symmetric informationally complete POVMs are complex projective 2-designs with angle set $\{1/(d+1)\}$.**

I. Introduction

Two quantum mechanical observables are called complementary if and only if precise knowledge of one of them implies that all possible outcomes are equally probable when measuring the other, see for example [19, p. 561]. The principle of complementarity was introduced by Bohr [6] in 1928, and it had a profound impact on the further development of quantum mechanics. A recent application is the quantum key exchange protocol by Bennett and Brassard [3] that exploits complementarity to secure the key exchange against eavesdropping.

We mention a simple mathematical consequence of this complementarity principle, which motivates some key notion. Suppose that O and O' are two hermitian $d \times d$ matrices representing a pair of complementary observables. We assume that the eigenvalues of both matrices are multiplicity free. It follows that the observables O and O' respectively have orthonormal eigenbases B and B' with basis vectors uniquely determined up to a scalar factor.

The complementarity of O and O' implies that if a quantum system is prepared in an eigenstate b' of the observable O', and O is subsequently measured, then the probability to find the system after the measurement in the state $b \in B$ is given by $|\langle b|b'\rangle|^2 = 1/d$. Recall that two orthonormal bases B and B' of $\mathbf{C}^d$ are said to be *mutually unbiased* precisely when $|\langle b|b'\rangle|^2 = 1/d$ holds for all $b \in B$ and $b' \in B'$. Thus the eigenbases of non-degenerate complementary observables are mutually unbiased. Conversely, we can associate to a pair of mutually unbiased bases a pair of non-degenerate complementary observables.

There is a fundamental property of mutually unbiased bases that is invaluable in quantum information processing. Suppose that we want to determine the density matrix ρ of an ensemble of quantum systems using as few non-degenerate observables as possible. We assume that it is possible to make a complete measurement of each observable $O = \sum_{b\in B} x_b\, |b\rangle\langle b\,|$, meaning that the statistics $\mathrm{tr}(\rho\, |b\rangle\langle b\,|) = \langle b|\,\rho\,|b\rangle$ is known for each eigenvalue x_b in the spectral decomposition. Ivanović showed in [12] that complete measurements of at least $d+1$ observables are needed to reconstruct the density matrix. He also showed that this lower bound is attained when $d+1$ non-degenerate pairwise complementary observables are used.

A simple example is provided by the Pauli spin matrices σ_x, σ_y, σ_z. A complete measurement of these three observables allows to reconstruct a 2×2 density matrix, a fact apparently known to Schwinger [18]. Nowadays, we know how to do this state tomography process—at least in principle—in dimensions $d = 3, 4$, and 5. It is an open problem whether it is possible to perform this kind of state tomography in dimension 6, because the construction of a set of 7 mutually unbiased bases in dimension $d = 6$ is elusive.

II. Mutually Unbiased Bases

Definition 1: Two orthonormal bases B and C of $\mathbf{C}^d$ are called mutually unbiased iff $|\langle b|c\rangle|^2 = 1/d$ holds for all $b \in B$ and $c \in C$.

The goal is to construct $d+1$ mutually unbiased bases (MUBs) in any dimension $d \geq 2$. There are several constructions known to obtain MUBs. At least for prime power dimension the problem is completely solved. This follows from Constructions I-III below. However, in any dimension other than a prime power it is unknown if a maximal set of $d+1$ MUBs can be found. The best known result is Construction IV below which only works in dimensions d which are squares and never gives a maximal set of MUBs.

Construction I (Wootters and Fields [24]) Let q be an odd prime power. Define

$$|v_{a,b}\rangle = q^{-1/2}(\omega_p^{\mathrm{tr}(ax^2+bx)})_{x\in\mathbb{F}_q} \in \mathbf{C}^q,$$

with $\omega_p = \exp(2\pi i/p)$. Then the standard basis together with the bases $B_a = \{|v_{a,b}\rangle\, | b \in \mathbb{F}_q\}$, $a \in \mathbb{F}_q$, form a set of $q+1$ mutually unbiased bases of $\mathbf{C}^q$.

Construction II (Galois Rings [13]) Let $\mathrm{GR}(4,n)$ be a finite Galois ring with Teichmüller set $\mathcal{T}_n$. Define

$$|v_{a,b}\rangle = 2^{-n/2}\left(\exp\left(\frac{2\pi i}{4}\mathrm{tr}(a+2b)x\right)\right)_{x\in\mathcal{T}_n}.$$

Then the standard basis together with the bases $M_a = \{|v_{a,b}\rangle \,|b \in \mathcal{T}_n\}$, $a \in \mathcal{T}_n$, form a set of 2^n+1 mutually unbiased bases of $\mathbf{C}^{2^n}$.

Construction III (Bandyopadhyay et al. [1]) Suppose there exist subsets $\mathcal{C}_1,\ldots,\mathcal{C}_m$ of a unitary error basis $\mathcal{B}$ such that $|\mathcal{C}_i| = d$, $\mathcal{C}_i \cap \mathcal{C}_j = \{\mathbf{1}_d\}$ for $i \neq j$, and the elements of $\mathcal{C}_i$ pairwise commute. Let M_i be a matrix which diagonalizes $\mathcal{C}_i$. Then $M_1,\ldots,M_m$ are MUBs.

Construction IV (Wocjan and Beth [23]) Suppose there are w mutually orthogonal Latin squares [4], each of size $d\times d$ over the symbol set $S = \{1,\ldots,d\}$. Then $w+2$ MUBs in dimension d^2 can be constructed as follows. With each Latin square L (and additionally the square $(1,2,\ldots,n)^t \otimes (1,\ldots,1)$) we can associate vectors of length d over the alphabet $\{1,\ldots,d^2\}$: for each symbol $\alpha\in S$ define a vector $s_{L,\alpha}\in\mathbf{C}^d$ as follows: start with the empty list $s_{L,\alpha}=\emptyset$. Then traverse the elements of L column-wise starting at the upper left corner. Whenever α occurs in position (i,j) in L, then append the number $i+jd$ to the list $s_{L,\alpha}$. The other ingredient to construct these MUBs is an arbitrary complex Hadamard matrix $H=(h_{i,j})$ of size $d\times d$. For each Latin square L and each $\alpha, j \in \{1,\ldots,d\}$ define a normalized vector $|v_{L,\alpha,j}\rangle := 1/\sqrt{d}\sum_{i=1}^d e_{s_{L,\alpha}[i]}h_{i,j}$, where e_i are the elementary basis vectors in $\mathbf{C}^{d^2}$. Then the bases given by $B_L := \{|v_{L,\alpha,j}\rangle : \alpha, j = 1,\ldots,d\}$ together with the identity matrix $\mathbf{1}_{d^2}$ form a set of $w+2$ MUBs.

Example 1: In dimension $d=3$ Construction I yields the bases

$$\begin{array}{llll}
3^{-1/2}\{ & (1,1,1), & (1,\omega_3,\omega_3^2), & (1,\omega_3^2,\omega_3)\},\\
3^{-1/2}\{ & (1,\omega_3,\omega_3), & (1,\omega_3^2,1), & (1,1,\omega_3^2)\},\\
3^{-1/2}\{ & (1,\omega_3^2,\omega_3^2), & (1,\omega_3,1), & (1,1,\omega_3)\},
\end{array}$$

which together with the standard basis $\mathbf{1}_3$ form a maximal system of four MUBs in $\mathbf{C}^3$.

Example 2: In dimension $d=4$ Construction II yields the bases (where we have abbreviated "$+$" for 1 and "$-$" for -1 and $i=\sqrt{-1}$):

$$\begin{array}{l}
\frac{1}{2}\{(+,+,+,+),(+,+,-,-),(+,-,-,+),(+,-,+,-)\},\\
\frac{1}{2}\{(+,-,-i,-i),(+,-,i,i),(+,+,i,-i),(+,+,-i,i)\},\\
\frac{1}{2}\{(+,-i,-i,-),(+,-i,i,+),(+,i,i,-),(+,i,-i,+)\},\\
\frac{1}{2}\{(+,-i,-,-i),(+,-i,+,i),(+,i,+,-i),(+,i,-,i)\}.
\end{array}$$

These four bases and the standard basis $\mathbf{1}_4$ form an extremal set of five MUBs in $\mathbf{C}^4$.

A basic question is how many bases can be achieved in general dimension. To this end, we define the function $M : \mathbf{N}\to\mathbf{N}$ as follows:

$$M(n) := \max\{|\mathcal{B}| :\ \mathcal{B} \text{ is a set of MUBs in } \mathbf{C}^n\}$$

Then we have that:

- $M(p^r) = p^r + 1$ for p prime, $r\in\mathbf{N}$,
- $M(n) \leq n+1$ for all $n\in\mathbf{N}$,
- $M(mn) \geq \min\{M(m), M(n)\}$ for all $m,n\in\mathbf{N}$.
- $M(d^2) \geq N(d)$, where $N(d)$ is the number of mutually orthogonal Latin squares of size $d\times d$.

An open problem is to show that $\liminf_{n\to\infty} M(n) = \infty$.

III. Welch's Lower Bounds

Suppose that X is a finite nonempty set of vectors of unit norm in the complex vector space $\mathbf{C}^d$. The vectors in X satisfy the inequalities

$$\frac{1}{|X|^2}\sum_{x,y\in X}|\langle x|y\rangle|^{2k} \geq \frac{1}{\binom{d+k-1}{k}}, \tag{1}$$

for all integers $k\geq 0$. Welch derived these bounds in [22] to obtain a lower bound on the maximal cross-correlation of spreading sequences of synchronous code-division multiple-access systems. Blichfeld [5] and Sidelnikov [20] derived similar bounds for real vectors of unit norm.

A set X attaining the Welch bound (1) for $k=1$ is called a WBE-sequence set, a notion popularized by Massey and Mittelholzer [15] and others. Using equation (1), it is straightforward to check that the union of $d+1$ mutually unbiased bases of $\mathbf{C}^d$ form a WBE-sequence set. These extremal sets of mutually unbiased bases are even better, since they also attain the Welch bound for $k=2$. In fact, we show that a sequence set attains the Welch bounds (1) for all $k\leq t$ if and only if it is a t-design in the complex projective space $\mathbf{C}P^{d-1}$.

Let us introduce some notation. Let S^{d-1} denote the sphere of unit vectors in the complex vector space $\mathbf{C}^d$. We say that two vectors u and v of S^{d-1} are equivalent, in signs $u\equiv v$, if and only if $u = e^{i\theta}v$ for some $\theta\in\mathbf{R}$. It is easy to see that $\equiv$ is an equivalence relation. We denote the quotient manifold $S^{d-1}/\!\equiv$ by $\mathbf{C}S^{d-1}$. Notice that the manifold $\mathbf{C}S^{d-1}$ is isomorphic to the complex projective space $\mathbf{C}P^{d-1}$, but we prefer the former notation because normalizing vectors to unit length is common practice in quantum computing.

Lemma 1: Let μ be the unique normalized $U(d)$-invariant Haar measure on the complex sphere $\mathbf{C}S^{d-1}$. For any $x\in S^{d-1}$, we have

$$\int_{\mathbf{C}S^{d-1}}|\langle x|y\rangle|^{2k}d\mu(y) = \frac{1}{\binom{d+k-1}{k}}.$$

Proof: The unitary group $U(d)$ acts transitively on the manifold $\mathbf{C}S^{d-1}$. This means that for any $y\in\mathbf{C}S^{d-1}$ there exists a unitary matrix U mapping y to the first basis vector, $Uy=e_1$. Therefore,

$$\begin{aligned}
\int_{\mathbf{C}S^{d-1}}|\langle x|y\rangle|^{2k}d\mu(x) &= \int_{\mathbf{C}S^{d-1}}|\langle Ux|e_1\rangle|^{2k}d\mu(x)\\
&= \int_{\mathbf{C}S^{d-1}}|\langle x|e_1\rangle|^{2k}d\mu(x),
\end{aligned}$$

where the last equality holds because of the $U(d)$-invariance of the measure μ. Using Proposition 1.4.9 from Rudin [17], we obtain

$$\int_{\mathbf{C}S^{d-1}} |\langle x|e_1\rangle|^{2k} d\mu(x) = \int_{\mathbf{C}S^{d-1}} |x_1^k|^2 d\mu(x) = \frac{1}{\binom{d+k-1}{d-1}},$$

which proves the claim. ■

IV. Complex Projective t-Designs

We now present some background material on complex projective designs. We will relate those later on to the systems of vectors formed by a maximal set of MUBs.

Let us first introduce some notation. We denote by $\mathrm{Hom}(k,\ell)$ the subset of the polynomial ring $\mathbf{C}[x_1,\dots,x_d,y_1,\dots,y_d]$ that consists of all polynomials that are homogeneous of degree k in the variables $x_1,\dots,x_d$ and homogeneous of degree ℓ in the variables $y_1,\dots,y_d$. We associate to each polynomial p in $\mathrm{Hom}(k,\ell)$ a function $p_\circ$ on the sphere S^{d-1} by defining $p_\circ(\xi) = p(\xi,\overline{\xi})$ for $\xi \in S^{d-1}$. The function $p_\circ$ is called the "restriction" of p onto the complex sphere. It follows from the homogeneity conditions of the polynomial p that $p_\circ(e^{i\vartheta}\xi) = e^{i\vartheta(k-\ell)}p_\circ(\xi)$ holds for all $\vartheta \in \mathbf{R}$. Therefore, we obtain a well-defined polynomial function on $\mathbf{C}S^{d-1}$ only if $k=\ell$. We define $\mathrm{Hom}(k,k)_\circ = \{p_\circ\colon p \in \mathrm{Hom}(k,k)\}$.

Definition 2: A finite nonempty subset X of $\mathbf{C}S^{d-1}$ is a t-design in $\mathbf{C}S^{d-1}$ iff the cubature formula

$$\frac{1}{|X|}\sum_{x\in X} f(x) = \frac{1}{\mu(\mathbf{C}S^{d-1})}\int_{\mathbf{C}S^{d-1}} f(x)d\mu(x)$$

holds for all f in $\mathrm{Hom}(t,t)_\circ$.

We now show a characterization of t-designs in terms of the inequalities by Welch given in equation (1).

Theorem 1: Suppose that X is a finite nonempty subset of $\mathbf{C}S^{d-1}$. Then the following statements are equivalent:

1) The set X is a t-design in $\mathbf{C}S^{d-1}$;
2) for all $x \in \mathbf{C}^d$ and all k in the range $0 \le k \le t$, we have the equality
$$\frac{\langle x|x\rangle^k}{\binom{d+k-1}{k}} = \frac{1}{|X|}\sum_{y\in X} |\langle x|y\rangle|^{2k}; \qquad (2)$$
3) the set X satisfies the Welch bounds (1) with equality for all k in the range $0 \le k \le t$, that is
$$\frac{1}{|X|^2}\sum_{x,y\in X} |\langle x|y\rangle|^{2k} = \frac{1}{\binom{d+k-1}{k}}, \qquad 0 \le k \le t. \qquad (3)$$

Proof: We show that 1) implies 2). Fix a vector $x \in \mathbf{C}^d$. Note that $p(y) = |\langle x|y\rangle|^{2k} = \langle y|x\rangle^k\langle x|y\rangle^k$ is a polynomial function in $\mathrm{Hom}(k,k)_\circ$. Since X is a t-design, the exact cubature formula

$$\frac{1}{|X|}\sum_{y\in X} |\langle x|y\rangle|^{2k} = \int_{\mathbf{C}S^{d-1}} |\langle x|y\rangle|^{2k} d\mu(y)$$

holds for all k in the range $0 \le k \le t$. By Lemma 1, the latter integral evaluates to $\binom{d+k-1}{k}^{-1}$, which proves that equation (2) holds for all $k \le t$.

We show next that 2) implies 3). We observe that (2) holds for all $k \le t$, hence summing over $x \in X$ yields (3).

Finally, we show that 3) implies 1). Suppose that equation (3) holds. For a vector $x \in \mathbf{C}^d$, we denote by $x^{\otimes k}$ the k-fold tensor product $x^{\otimes k} = x \otimes \cdots \otimes x \in \mathbf{C}^{d^k}$. Note that $\langle x^{\otimes k}|y^{\otimes k}\rangle = \langle x|y\rangle^k$. Consider the d^{2k}-dimensional vector

$$\xi = \frac{1}{|X|}\sum_{x\in X} x^{\otimes k}\otimes \overline{x}^{\otimes k} - \int_{\mathbf{C}S^{d-1}} x^{\otimes k}\otimes\overline{x}^{\otimes k} d\mu(x).$$

Evaluating the inner product of ξ with itself yields

$$\frac{1}{|X|^2}\sum_{x,y\in X} |\langle x|y\rangle|^{2k} - \int\int_{\mathbf{C}S^{d-1}} |\langle x|y\rangle|^{2k} d\mu(y)d\mu(x), \quad (4)$$

which is equal to $\langle \xi|\xi\rangle \ge 0$. The inner integral evaluates to $\binom{d+k-1}{k}^{-1}$ by Lemma 1, and the double integral has the same value, because the measure μ is normalized. It follows from our assumption that the right hand side vanishes. By construction of ξ, we can conclude that averaging over X yields an exact cubature formula for all monomials in $\mathrm{Hom}(k,k)_\circ$, hence, by linearity, for all polynomials in $\mathrm{Hom}(k,k)_\circ$. This means that X is a t-design. ■

Remark 1: Equation (4) provides a short proof of the Welch inequalities (1). The analogue for real spherical t-designs of the above result is sketched in [7]. A connection to the existence of certain isometric Banach space embeddings is given in [14].

V. Uniform Tight Frames

A finite subset F of nonzero vectors of $\mathbf{C}^d$ is called a frame if there exist nonzero real constants A and B such that

$$A\|v\|^2 \le \sum_{f\in F} |\langle f|v\rangle|^2 \le B\|v\|^2$$

holds for all $v \in \mathbf{C}^d$. The notion of a frame generalizes the concept of an orthonormal basis. The linear span of the vectors in F the space $\mathbf{C}^d$, but the vectors in a frame are in general not linearly independent. A frame is called tight if and only if the frame bounds A and B are equal. A tight frame is called isometric (or uniform) if and only if each vector in F has unit norm.

Theorem 2: Let F be a finite nonempty subset of vectors in $\mathbf{C}^d$. The following statements about F are equivalent:

1) F is a uniform tight frame;
2) F is a WBE-sequence set;
3) F is a 1-design in $\mathbf{C}S^{d-1}$.

Proof: The frame constants of a uniform tight frame F in $\mathbf{C}^d$ are given by $A = B = |F|/d$, see for example Property 2.3 in [8]. Therefore, F satisfies equation (2) of Theorem 1 for $k=1$. The equivalence of the three statements follow now from Theorem 1. ■

Corollary 1: Any 1-design in $\mathbf{C}P^{d-1}$ is obtained by projecting an orthogonal basis from a higher-dimensional space (where all basis vectors have the same norm).

VI. Equivalence of MUBs and 2-Designs

We need a few more notations before we state our main results. If $\mathcal{B}$ is a subset of $\mathbf{C}S^{d-1}$, then the set $A = \{|\langle x|y\rangle|^2 \colon x, y \in \mathcal{B}, x \neq y\}$ is called the "angle" set of $\mathcal{B}$. For an element x in $\mathcal{B}$ and an "angle" $\alpha \in A$, we define the subdegree $d_\alpha(x)$ as $d_\alpha(x) = |\{y \in \mathcal{B} \colon |\langle x|y\rangle|^2 = \alpha\}|$. If the subdegree d_α of an $\alpha \in A$ is independent of x, then $\mathcal{B}$ is called a *regular scheme*. Note that the union of mutually orthogonal bases of $\mathbf{C}^d$ is a regular scheme with angle set $\{0, 1/d\}$.

Theorem 3: The union X of $d+1$ mutually unbiased bases in $\mathbf{C}^d$ forms a 2-design in $\mathbf{C}S^{d-1}$ with angle set $\{0, 1/d\}$ and $d(d+1)$ elements.

Proof: We verify that X attains the Welch bound in equation (1) with equality for $0 \leq k \leq 2$. The statement then follows from Theorem 1. Indeed, this is obvious for $k = 0$. We note that $|X| = d(d+1)$.

If we evaluate the left hand side of the Welch bound for X, then we obtain

$$\begin{aligned}\frac{1}{d^2(d+1)^2}\sum_{x,y\in X}|\langle x|y\rangle|^2 &= \frac{d(d+1)}{d^2(d+1)^2}\left(1+(d-1)0+d^2\frac{1}{d}\right)\\ &= \frac{1}{d}\end{aligned}$$

and this coincides with $\binom{d+1-1}{1}^{-1} = 1/d$; so, X is a 1-design. Similarly, for $k = 2$,

$$\begin{aligned}\frac{1}{d^2(d+1)^2}\sum_{x,y\in X}|\langle x|y\rangle|^4 &= \frac{d(d+1)}{d^2(d+1)^2}\left(1+(d-1)0+d^2\frac{1}{d^2}\right)\\ &= \frac{2}{d(d+1)},\end{aligned}$$

and this coincides with $\binom{d+2-1}{2}^{-1} = 2/(d(d+1))$. ■

Theorem 4: A 2-design $\mathcal{B}$ in complex projective space $\mathbf{C}S^{d-1}$ with angle set $\{0, 1/d\}$ and $|\mathcal{B}| = d(d+1)$ elements is the union of $d+1$ mutually unbiased bases.

Proof: A complex projective 2-design with $s = |\{0, 1/d\}| = 2$ satisfies $2 \geq s-1$, hence is a regular scheme [10]. For $\alpha = 1/d$, any $x \in \mathcal{B}$ has subdegree $d_\alpha(x) = d^2$ by Theorem 2.5 of [10]. It follows that x is orthogonal to $d-1$ elements.

Let $B_x = \{x\} \cup \{z \in \mathcal{B} \colon \langle x|z\rangle = 0\}$. We claim that B_x is an orthonormal basis of $\mathbf{C}^d$. We may assume that the vectors in $\mathcal{B}$ are normalized to unit norm. Thus, it suffices to show that $B_x = B_y$ for each $y \in B_x$. For $x = y$ this is trivial. We know that x and y are contained in both B_x and B_y. Therefore, it suffices to show that the intersection set

$$I(x,y) = \{z \in \mathcal{B} \colon \langle x|z\rangle = 0, \langle y|z\rangle = 0\} = B_x \cap B_y - \{x, y\}$$

contains $d-2$ elements.

The number of elements in $I(x,y)$ does not depend on x, y for a t-design with $t \geq 2s-2$, see [11]. Specializing Theorem 5.2 in [11] to the case at hand shows that

$$|I(x,y)| = d^2\sum_{i,j=0}^{1}\sigma^0_{1-i}\sigma^0_{1-j}\big(d(d+1)g_{ij}(0) - 0^i - 0^j\big).$$

We can now evaluate the intersection polynomials $g_{ij}(0)$ using [11, Theorem 5.3] and obtain that $|I(x,y)| = d-2$.

Hence we can conclude that each set B_x forms an orthonormal basis of $\mathbf{C}^d$. The sets B_x partition $\mathcal{B}$. If $B_x \neq B_z$, then the bases are by construction mutually unbiased. ■

Zauner conjectures that if the dimension d is not a prime power, then a 2-design with angle set $\{0, 1/d\}$ cannot have $d(d+1)$ elements [25]. His conjecture can now be reformulated in terms of mutually unbiased bases, which then states that $N(d) < d+1$ for non-prime power d. If Zauner's conjecture is true, then this would explain the particular role of the finite field construction by Wootters and Fields [24].

Remark 2: Theorem 3 was obtained earlier by Zauner as part of a more general result on combinatorial quantum designs using a different terminology, see [25, Theorem 2.19]. The converse direction, our Theorem 4, appears to be new.

VII. SIC-POVMs and 2-Designs

Finally, to demonstrate the versatility of Theorem 1 we also show that another system of vectors used in quantum information theory corresponds to complex projective 2-designs. So-called symmetric informationally complete positive operator-valued measures (SIC-POVMs) are systems of d^2 vectors in $\mathbf{C}^d$ which have constant inner product, i. e., $|\langle v, w\rangle|^2 = 1/(d+1)$ for all v, w in the set. Like in case of MUBs it is a challenging task to construct SIC-POVMs—indeed here solutions are known only for a finite number of dimensions [9], [16]. In [16] it was shown that SIC-POVMs actually form complex projective 2-designs. The following theorem gives a new and simple proof of this result.

Theorem 5 (SIC-POVMs are 2-designs [16]): Let X be a SIC-POVM X in dimension d. Then X forms a 2-design in $\mathbf{C}S^{d-1}$ with angle set $\{1/(d+1)\}$ and d^2 elements.

Proof: Again, we only have to verify that the set X of vectors attains the Welch bound with equality for $0 \leq k \leq 2$. The statement then follows from Theorem 1. Indeed, this is obvious for $k = 0$. We note that here $|X| = d^2$. Evaluating the left hand side of the Welch bound for X, then we obtain

$$\begin{aligned}\frac{1}{d^4}\sum_{x,y\in X}|\langle x|y\rangle|^2 &= \frac{1}{d^4}\left(d^2\cdot 1+(d^4-d^2)\frac{1}{d+1}\right)\\ &= \frac{1}{d^2}\left(1+(d-1)\right) = \frac{1}{d}\end{aligned}$$

and this coincides with $\binom{d+1-1}{1}^{-1} = 1/d$; so, X is a 1-design. Similarly, for $k = 2$,

$$\begin{aligned}\frac{1}{d^4}\sum_{x,y\in X}|\langle x|y\rangle|^4 &= \frac{1}{d^4}\left(d^2\cdot 1+(d^4-d^2)\frac{1}{(d+1)^2}\right)\\ &= \frac{1}{d^2}\left(1+\frac{d-1}{d+1}\right) = \frac{2}{d(d+1)}\end{aligned}$$

and this coincides with $\binom{d+2-1}{2}^{-1} = 2/(d(d+1))$. ■

Remark 3: Zauner pointed out to us that the previous theorem can also be obtained in the language of combinatorial quantum designs by combining Theorems 2.29 and 2.30 in his dissertation [25].

VIII. Conclusion

We have shown that the seemingly unrelated concepts of MUBs on the one hand and complex projective 2-deigns on the other are actually the same objects. This was anticipated in a paper by Barnum [2] in which it was shown that the union of the (d+1) bases of a particular system of MUBs forms a complex projective 2-design. In the present paper we have generalized this to arbitrary MUBs and have also shown the other direction, i. e., any 2-design in dimension d which consists of $d^2 + d$ elements and has angle set $\{0, 1/d\}$ can be partitioned into $d+1$ sets of MUBs. We have also shown that these sets meet the Welsh bounds for $k = 0, 1, 2$ with equality. Hence, the present paper can also be seen as a generalization of the results of [21] in which the corresponding statement over the real numbers was shown. Finally, we would like to mention that Zauner [25] conjectures that affine 2-designs do not exist in dimensions d having two distinct prime factors.

Acknowledgment

We are grateful to Emina Soljanin for bringing tight frames to our attention, and to Gerhard Zauner for assisting with the translation of his results. We also thank Chris Godsil, Markus Grassl, Joe Renes, Aidan Roy for several interesting discussions, and Richard Cleve for pointing out a small error in an example of a previous version.

The research of A.K. was supported in part by NSF grant CCR-0218582, NSF CAREER award CCF-0347310, a TEES Select Young Faculty award, and a Texas A&M TITF grant. This work was carried out while M.R. was at the Institute for Quantum Computing, University of Waterloo, Canada.

References

[1] S. Bandyopadhyay, P. O. Boykin, V. Roychowdhury, and F. Vatan. A new proof for the existence of mutually unbiased bases. *Algorithmica*, 34:512–528, 2001.

[2] H. Barnum. Information-disturbance tradeoff in quantum measurement on the uniform ensemble and on the mutually unbiased bases. ArXiv preprint quant–ph/0205155, 2002.

[3] C.H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proc. of the IEEE Intl. Conf. Computers, Systems, and Signal Processing*, pages 175–179. IEEE, 1984.

[4] Th. Beth, D. Jungnickel, and H. Lenz. *Design Theory*, volume I. Cambridge University Press, 2. edition, 1999.

[5] H.F. Blichfeld. The minimum value of quadratic forms, and the closest packing of spheres. *Math. Ann.*, 101:605–608, 1929.

[6] N. Bohr. Das Quantenpostulat und die neueren Entwicklungen der Atomistik. *Naturwissenschaften*, 16:245–257, 1928.

[7] J.M. Goethals and J.J. Seidel. Cubature formulae, polytopes, and spherical designs. In C. Davis, B. Grünbaum, and F.A. Sherk, editors, *The Geometric Vein – The Coxeter Festschrift*, pages 203–218. Springer-Verlag, 1981.

[8] V.K. Goyal, J. Kovačevič, and J.A. Kelner. Quantized frame expansions with erasures. *Appl. Comp. Harm. Analysis*, 10:203–233, 2001.

[9] M. Grassl. On SIC-POVMs and MUBs in Dimension 6. pages 60–61. Proceedings ERATO Conference on Quantum Information Science (EQIS 2004), Tokyo, 2004. See also ArXiv preprint quant-ph/0406175.

[10] S.G. Hoggar. Parameters of t-designs in $\mathbb{F}P^{n-1}$. *Europ. J. Combin.*, 5:29–36, 1984.

[11] S.G. Hoggar. t-designs with general angle set. *Europ. J. Combin.*, 13:257–271, 1992.

[12] I. D. Ivanovic. Geometrical description of quantal state determination. *Journal of Physics A*, 14(12):3241–3245, 1981.

[13] A. Klappenecker and M. Rötteler. Constructions of mutually unbiased bases. volume 2948 of *LNCS*, pages 137–144. Springer, 2004.

[14] H. König. Isometric embeddings of Euclidean spaces into finite dimensional ℓ_p-spaces. In B. Jakubczyk, S. Janeczko, and B. Ziemian, editors, *Panoramas of Mathematics*, volume 34 of *Banach Center Publications*, pages 79–87, Warsaw, 1995.

[15] J.L. Massey and T. Mittelholzer. Welch's bound and sequences sets for code-division multiple-access systems. In *Sequences II: Methods in Communications, Security and Computer Sciences*, pages 63–78, Heidelberg, 1993. Springer-Verlag.

[16] J. M. Renes, R. Blume-Kohout, A. J. Scott, and C. M. Caves. Symmetric informationally complete quantum measurements. *J. Math. Phys*, 45(6):2171–2180, 2004.

[17] W. Rudin. *Function Theory in the Unit Ball of* $\mathbf{C}^n$. Springer-Verlag, New York, 1980.

[18] J. Schwinger. Unitary operator bases. *Proc. Nat. Acad. Sci. U.S.A.*, 46:570–579, 1960.

[19] M.O. Scully and M.S. Zubairy. *Quantum Optics*. Cambridge University Press, Cambridge, 1997.

[20] V.M. Sidelnikov. New bounds for the density of sphere packings in an n-dimensional Euclidean space. *Mat. Sbornik* 95 (1974) = *Math. USSR Sbornik*, 24:147–157, 1974.

[21] S. Waldron. Generalized Welch bound equality sequences are tight frames. *IEEE Transactions on Information Theory*, 49(9):2307–2309, 2003.

[22] L.R. Welch. Lower bounds on the maximum cross correlation of signals. *IEEE Transactions on Information Theory*, 20(3):397–399, 1974.

[23] P. Wocjan and Th. Beth. New construction of mutually unbiased bases in square dimensions. ArXiv preprint quant–ph/0407081, 2004.

[24] W. Wootters and B. Fields. Optimal state-determination by mutually unbiased measurements. *Ann. Physics*, 191(2):363–381, 1989.

[25] G. Zauner. *Quantendesigns – Grundzüge einer nichtkommutativen Designtheorie (in German)*. PhD thesis, Universität Wien, 1999.